

# Edge Management Service:

Modern Cross Platform Browser Management



# Speakers



**Jörgen Nilsson**

Trusted Advisor

 [in/ccmexec/](https://www.linkedin.com/in/ccmexec/)



**Matthew Teegarden**

 [in/matthewteegarden/](https://www.linkedin.com/in/matthewteegarden/)



**Sandy**

Senior Cloud Architect

 [in/sandy-tsang/](https://www.linkedin.com/in/sandy-tsang/)

Can't see our slides? Can't hear? Need to repeat the question? Call us out!

# Agenda

- Introduction
- Edge Management Service
- Extensions
- Security Baselines
- Migration from Intune/Group Policy
- Multi-platform support
- External scenarios
- What about Google Chrome?
- Summary



# Browsers – our most important app

- ◆ Number of SaaS applications used per organization has increased every year, but we are seeing consolidation of SaaS apps as a trend.
- ◆ With SaaS apps becoming increasingly important when CRM, Finance and many other systems moved to the Web, Browser security is more important than ever!
- ◆ How is our browser secured?
- ◆ BYOD access to webapps?
- ◆ How are they secured?
- ◆ Extensions how secure are they?



# Browser strategy

From ServiceDesk ticket:

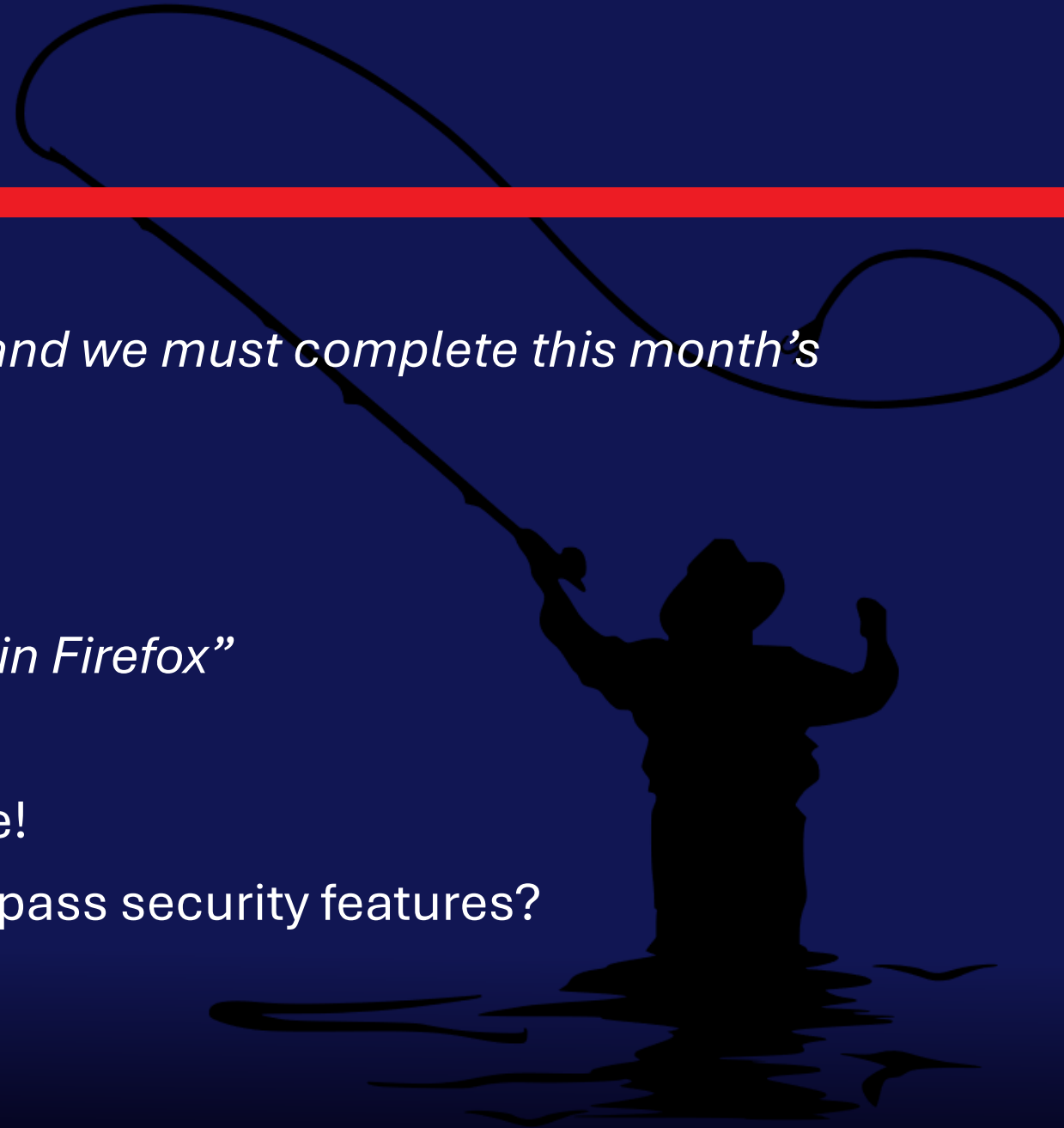
*“The xxx webpage doesn’t work in Edge and we must complete this month’s salary payment ASAP”*

Customer update:

*“This is not urgent anymore as it worked in Firefox”*

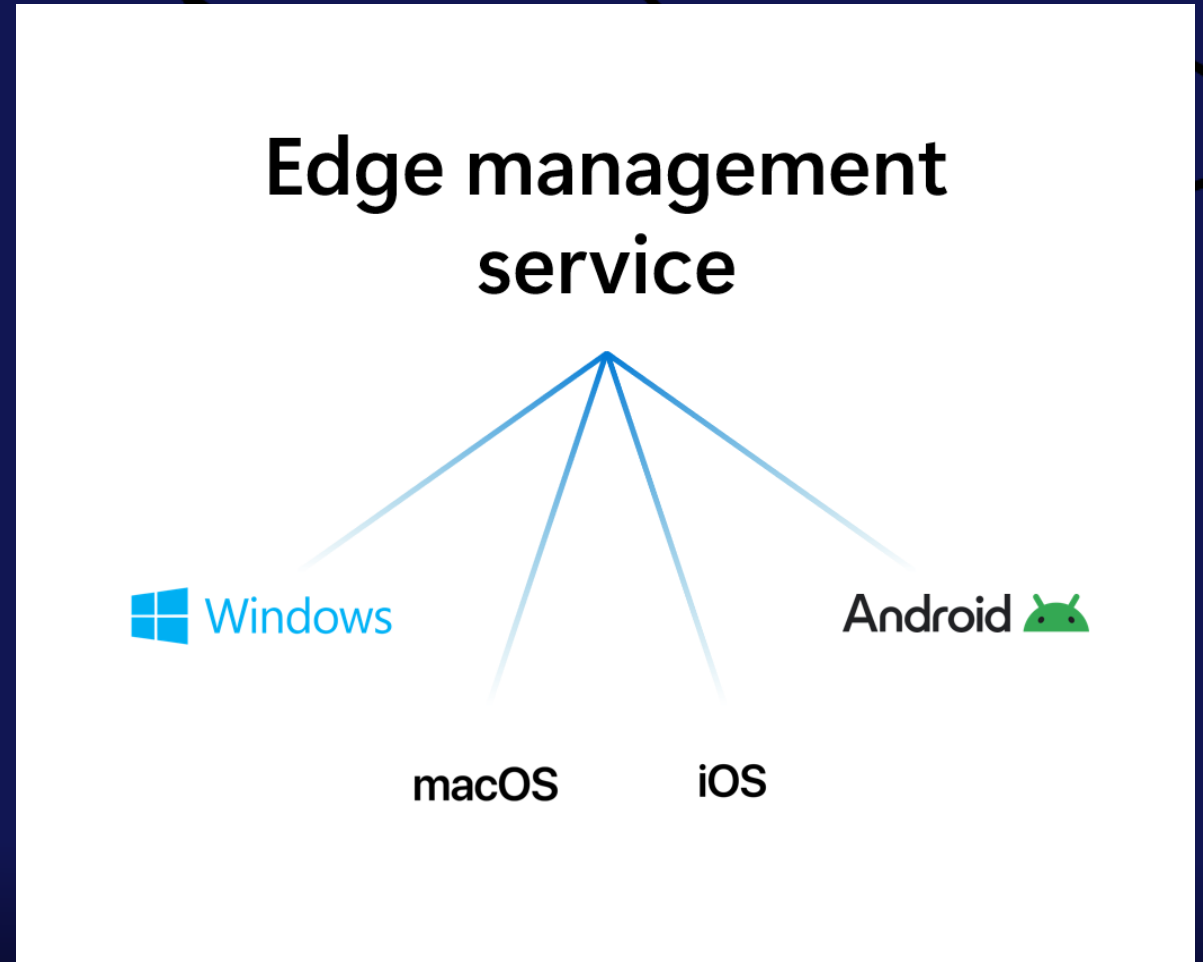
The root cause was an expired certificate!

◆ How secure is Firefox when you can bypass security features?



# Multiplatform support (February 2026)

- ◆ Windows, Android, macOS, iOS
- ◆ Zero-day support for settings
- ◆ Consistency
- ◆ Timesaving



# What is Edge Management Service & Why It Exists



# The Browser Management Challenge

## Traditional Challenges

- ◆ Multi-platform environments (Windows, macOS, iOS, Android)
- ◆ BYOD and unmanaged devices (can't use GPO or Intune MDM)
- ◆ Policy lag (waiting for Intune updates to support new Edge settings)
- ◆ User mobility (policies should follow users across devices)
- ◆ Visibility gaps (hard to see Edge health, extensions, versions)

**Modern Need: Cloud-native, user-centric, real-time management**

# What is Microsoft Edge Management Service

- Cloud-based browser management platform (part of M365)
- Managed via Microsoft 365 Admin Center
- Microsoft Edge Administrator - Role
- Supports user-based (group assignment) and device-based (enrollment token) targeting
- A single pane of glass for Edge management Cloud+Intune
- Includes extension management, reporting, security insights
- Priority !
- Zero-day support for new Edge settings (no waiting for Intune updates)

<input type="checkbox"/>	NA	Win - Conflict 2
<input type="checkbox"/>	NA	Win - Conflict 1
<input type="checkbox"/>	NA	Edge conflict
<input type="checkbox"/>	0	Security Baseline
<input type="checkbox"/>	1	Security Settings
<input type="checkbox"/>	2	Edge Standard
<input type="checkbox"/>	3	Security baseline v128
<input type="checkbox"/>	4	Edge Demo
<input type="checkbox"/>	5	Show Home button
<input type="checkbox"/>	6	Monitoring Policy This policy was auto-created from the monitoring page policy, visit the monitoring page.
<input type="checkbox"/>	7	Configure Extensions
<input type="checkbox"/>	8	Purview browser protections policy for Unmanaged blocks other non-compliant browsers

# Monitoring (Default)

## Policies for Microsoft Edge

Overview Configuration policies Site lists Connectors **Monitoring dashboard**

 Provide Feedback

 **Devices recommended to update**

**10** out of 11

 **Requested extensions**

**8**

 **Requested IE mode sites**

**0**

Ensuring all devices are running the latest Edge version improves your overall security posture. The following tables provide details about Edge versions running in your organization and actions you can take to keep them up to date. View these details by turning on the toggle to enable version monitoring. Note: If you have set [Edge update policies](#) for your organization, this feature may not work as expected.

Enable version monitoring

### Edge version management

...

#### Edge update status

*11 total managed devices, 1 devices sending data in the last 24 hours.*

Devices without the latest Edge updates may be vulnerable. We recommend restarting these instances to apply the latest browser version. In the event of an unpatched zero-day incident, we strongly suggest restarting the browser as soon as a [security update is released](#).









Updated at September 8, 2025 at 9:38 PM today



■ Up To Date ■ Update Available ■ Update Recommended

# Org settings

Services   Security & privacy   Organization profile

Name ↑	Description
 Custom themes	Customize Microsoft 365 for your organization.
 Custom tiles for Apps	Add tiles that open websites or SharePoint sites.
 Data location	See where Microsoft stores your data for your organization.
 Help desk information	Streamline user support by adding custom help desk information.
 Keyboard shortcuts	Perform many common tasks using the keyboard (e.g., Ctrl+K).
 Multitenant collaboration	Enable users in your multitenant organization to collaborate.
 Organization information	Update your organization's contact info, such as name and address.
 Release preferences	Choose how your organization gets new features and service updates from Microsoft 365.

## Release preferences

Choose how your organization gets new features and service updates from Microsoft 365.

[Learn more about release validation at Microsoft](#)

This setting doesn't affect how Microsoft 365 apps, such as Word and Excel, get new features and updates. To choose when Microsoft 365 apps get new features and updates, go to [Microsoft 365 installation options](#).

- Standard release for everyone  
Your entire organization gets updates when we release them broadly.
- Targeted release for everyone  
Your entire organization gets updates early.
- Targeted release for select users  
Pick people to receive updates early to preview them before they're released to everyone else.

Save

# Targeted release (Organizational setting)

Home > Microsoft Edge for Business

## Microsoft Edge for Business

[Monitoring dashboard](#) Configuration policies Site lists Connectors Copilot Resources

[Provide Feedback](#)

### Extensions Monitoring

Requested extensions

1

[Go to Extensions](#)

### Security Insights: Edge Update Status

**9/15 devices recommended to update.**

To apply the latest Edge version, restart your devices. If an unpatched zero-day incident occurs, we recommend restarting your browser as soon as a security update is available.

#### Edge Updates



Last updated 8:28 PM today

Edge channel	Total devices	▲ Update available	▲ Update recommended
> Stable ⓘ	9	▲ 2	▲ 3

[Force auto restart when device is idle](#)

[Recommend restart](#)

### Flight prerelease channels

To prepare for each new major version of Edge, we suggest flying Edge prerelease channels inside the stable Edge application to a select group in your organization. Require your end-users to use the selected

# Microsoft Edge for Business

Extensions monitoring ▾

Configuration policies

Site lists

Connectors

Copilot

Resources


 Provide Feedback

*Note: We have recently updated this page to aggregate all extension requests. You may temporarily see previously resolved requests.*

 Export

13 items

 Filter ▾

 Search

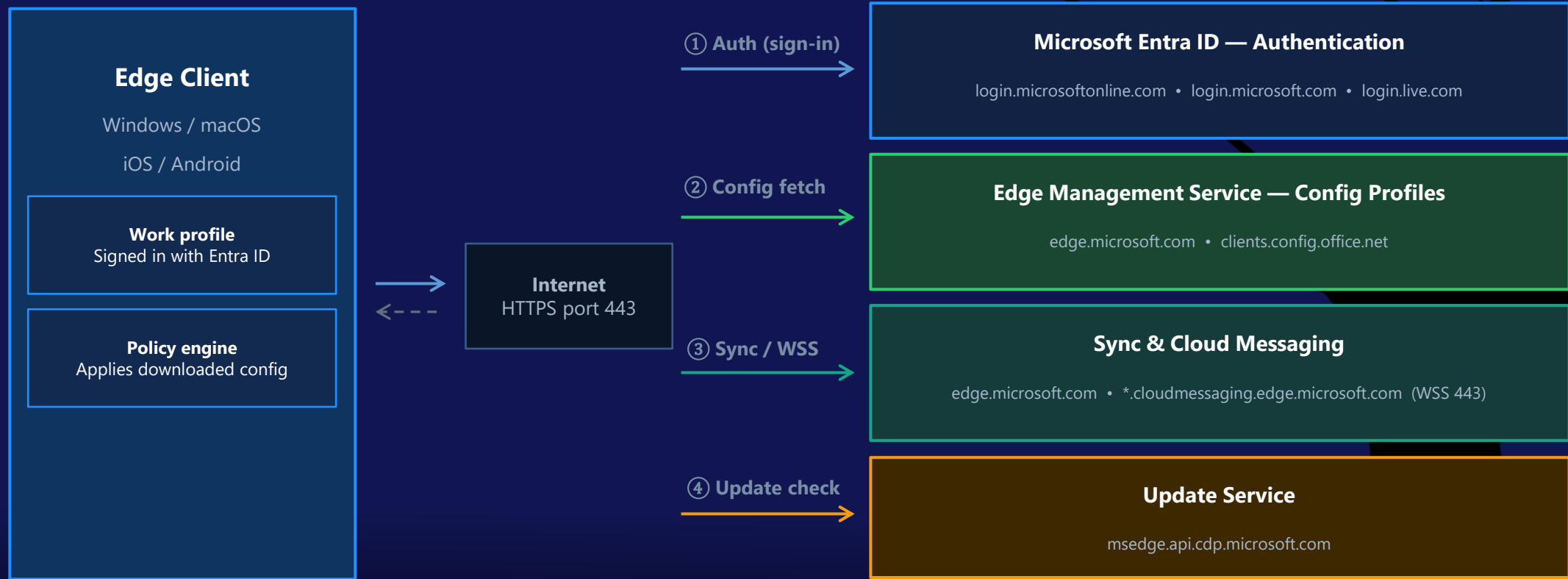
Active extension requests - 13

Extension name ↑	Type	Users with extension installed	Number of requests
<a href="#">AdBlock — block ads across the web</a>	Edge Add-on	0	1
<a href="#">AdBlocker Ultimate</a>	Edge Add-on	0	1
<a href="#">AI Grammar Checker &amp; Paraphraser – LanguageTool</a>	Edge Add-on	0	1
<a href="#">Holiday Snowman</a>	Edge Add-on	0	1
<a href="#">LastPass: Free Password Manager</a>	Edge Add-on	0	1
<a href="#">LinkedIn Extension</a>	Edge Add-on	0	2
<a href="#">Malwarebytes Browser Guard</a>	Edge Add-on	0	1
<a href="#">Microsoft 50th Anniversary – Celebration</a>	Edge Add-on	0	2
<a href="#">Microsoft Bing Homepage and Search Engine</a>	Edge Add-on	0	1



# Edge Client → Edge Management Service

## Traffic Flow & Required Endpoints



→ Authentication flow

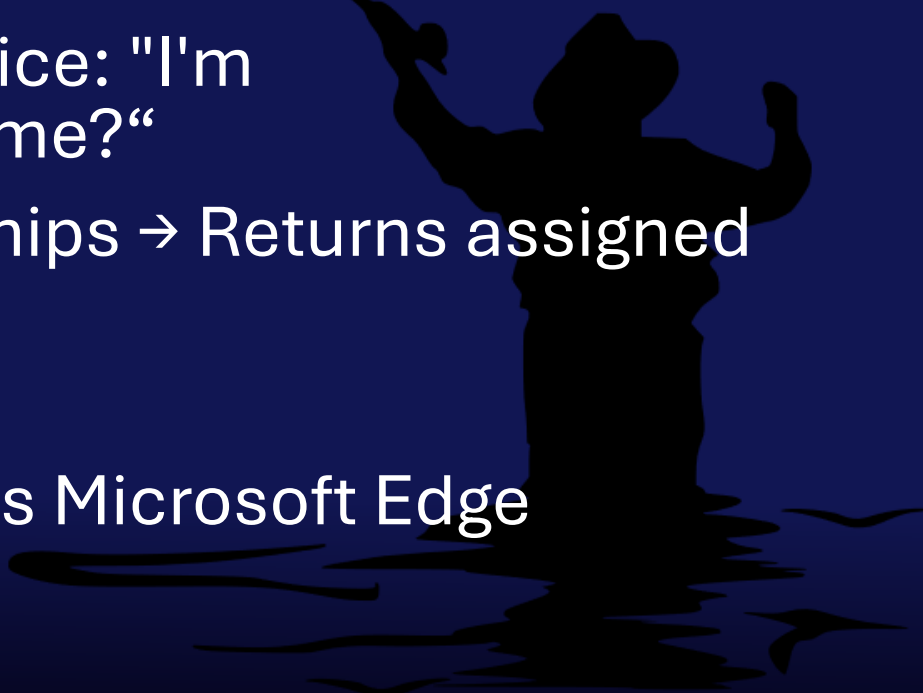
→ Config / sync (HTTPS 443)

→ Update check

- - - - -> Response / return

# Policy Delivery Flow (User-Based)

1. Admin creates cloud policy in M365 Admin Center
2. Admin assigns policy to Microsoft Entra user groups
3. User signs into Edge with work account (e.g., [user@mmsmoa.com](mailto:user@mmsmoa.com))
4. Edge contacts Edge Management Service: "I'm [user@mmsmoa.com](mailto:user@mmsmoa.com), any policies for me?"
5. Service checks user's group memberships → Returns assigned policies
6. Edge applies policies locally
7. Take effect the next time the user opens Microsoft Edge



# Monitoring Policy

## Properties

### Basics

Name	Monitoring Policy
Description	This policy was auto-created from the monitoring page. To delete this policy, visit the monitoring page.
Policy type	Cloud
Platforms	<span>Windows</span> <span>macOS</span> <span>iOS</span> <span>Android</span>

### Settings

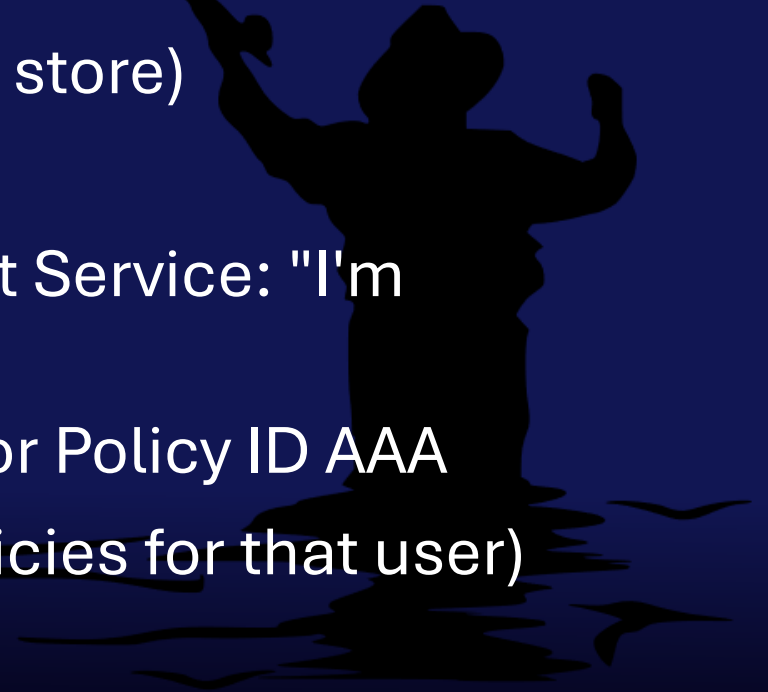
Name	Configuration	User override	Applies to
<b>CloudReportingUploadFrequency</b> Frequency of cloud reporting in hours	3	Not Allowed	<span>Windows</span>
<b>CloudProfileReportingEnabled</b> Enable Microsoft Edge cloud reporting for managed profile	Enabled	Not Allowed	<span>Windows</span>
<b>ForceDiagnosticData</b>	[[{"name": "value", "value": "2"}]]	Not Allowed	<span>Windows</span>

### Assignments

Group	Description
All users	This configuration applies to all users in the tenant

# Policy Delivery Flow (Device-Based via Token)

1. Admin creates cloud policy in M365 Admin Center
2. Admin copies Policy ID (enrollment token)
3. Admin deploys token via Intune or GPO (EdgeManagementEnrollmentToken)
4. Device receives token (written to registry/policy store)
5. User signs into Edge on that device
6. Edge reads token → Contacts Edge Management Service: "I'm enrolled with Policy ID AAA"
7. Service returns the cloud policy configuration for Policy ID AAA
8. Edge applies device-level policy (+ any user policies for that user)



# Edge Enrollment Token

Creates cloud policy in M365 Admin Center

Home > Microsoft Edge for Business

## Microsoft Edge for Business

Dashboard ▾ **Configuration policies** Site lists Connectors Copilot Resources

 Provide Feedback

Manage browser settings for your organization with configuration policies. If a user is assigned to multiple policies with conflicting settings, then the setting of the highest priority policy is applied.

[+ Create policy](#) [↻ Refresh](#)



Priority ↓	Name	Policy type	Scope	Platforms	Last modified date	Modified by
<input type="checkbox"/> 1	Disable Home button	Cloud	Tenant	<span>Windows</span> <span>macOS</span> <span>iOS</span> <span>Android</span>	2026-04-28	Admin MVP24
<input type="checkbox"/> 0	Monitoring Policy <small>This policy was auto-created from the monitoring page. To delete this policy, visit the monitoring page.</small>	Cloud	Tenant	<span>Windows</span> <span>macOS</span> <span>iOS</span> <span>Android</span>	2026-04-28	Admin MVP24

# Edge Enrollment Token

## ◆ Deploy Policy ID (enrollment token)

Home > Microsoft Edge for Business

## Microsoft Edge for Business

Dashboard ▾ Configuration policies Site lists Connectors Copilot Resources

 Provide Feedback

Manage browser settings for your organization with configuration policies. If a user is assigned to multiple policies with conflicting settings, then the setting of the highest priority policy is applied.

 Delete policy  Copy policy  Import  Export policy  Reorder priority  Deploy 

	Priority ↓	Name	Policy type	Scope	Platforms	Last modified date	Modified by
<input checked="" type="checkbox"/>	1	Disable Home button	Cloud	Tenant	Windows macOS iOS Android	2026-04-28	Admin MVP24
<input type="checkbox"/>	0	Monitoring Policy <small>This policy was auto-created from the monitoring page. To delete this policy, visit the monitoring page.</small>	Cloud	Tenant	Windows macOS iOS Android	2026-04-28	Admin MVP24

# Edge Enrollment Token

## ◆ Copies Policy ID (enrollment token)

Home > Microsoft Edge for Business

## Microsoft Edge for Business

Dashboard ▾ Configuration policies Site lists Connectors Copilot Resources

Manage browser settings for your organization with configuration policies. If a user is assigned to multiple policies with conflicting settings, then the setting of the highest priority policy is applied.

 Delete policy  Copy policy  Import  Export policy  Reorder priority  Deploy

	Priority ↓	Name	Policy type	Scope	Platforms
<input checked="" type="checkbox"/>	1	Disable Home button	Cloud	Tenant	Windows macOS iOS
<input type="checkbox"/>	0	Monitoring Policy <small>This policy was auto-created from the monitoring page. To delete this policy, visit the monitoring page.</small>	Cloud	Tenant	Windows macOS iOS


### Deploy configuration profile

Select one or more existing configuration policies from Intune to deploy this profile to. Deploying this profile may overwrite any existing configuration for the EdgeManagementEnrollmentToken policy.

If you want to deploy this profile using group policy, then copy the profile ID to use as the value for the EdgeManagementEnrollmentToken policy.

#### Configuration policy

Select a profile ▾

 Copy Profile ID

# Edge Enrollment Token

- ◆ Copies Policy ID (enrollment token)

Home > Microsoft Edge for Business

## Microsoft Edge for Business

Dashboard ▼ Configuration policies Site lists Connectors Copilot Resources

Manage browser settings for your organization with configuration policies. If a user is assigned to multiple policies with conflicting settings, then the setting of the highest priority policy is applied.

 Delete policy  Copy policy  Import  Export policy  Reorder priority  Deploy

	Priority <span>↓</span>	Name	Policy type	Scope	Platforms
<input checked="" type="checkbox"/>	1	Disable Home button	Cloud	Tenant	Windows macOS iOS
<input type="checkbox"/>	0	Monitoring Policy <small>This policy was auto-created from the monitoring page. To delete this policy, visit the monitoring page.</small>	Cloud	Tenant	Windows macOS iOS

### Deploy configuration profile ✕

Select one or more existing configuration policies from Intune to deploy this profile to. Deploying this profile may overwrite any existing configuration for the EdgeManagementEnrollmentToken policy.

If you want to deploy this profile using group policy, then copy the profile ID to use as the value for the EdgeManagementEnrollmentToken policy.

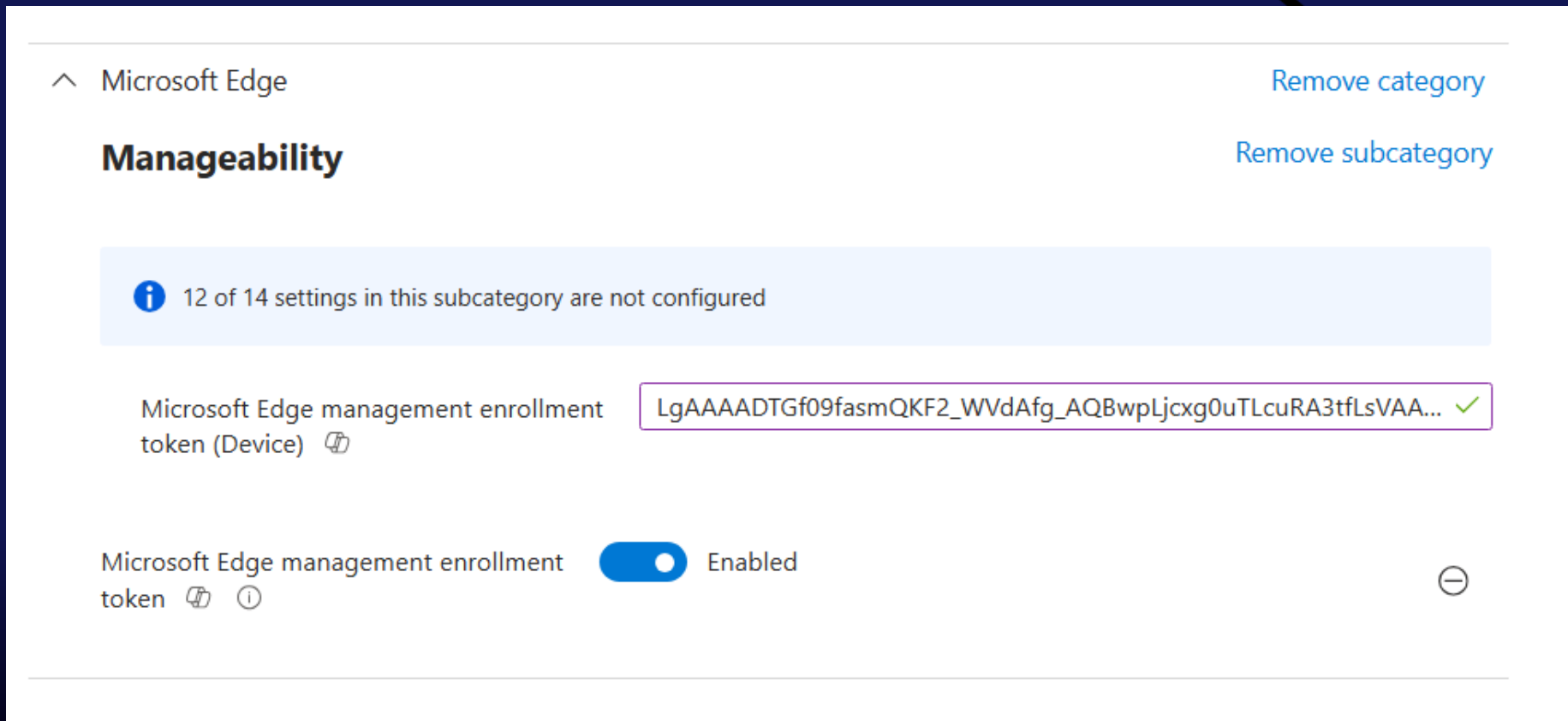
#### Configuration policy

Select a profile ▼

 Profile ID Copied!

# Edge Enrollment Token

- ◆ Deploys token via Intune



Microsoft Edge Remove category

**Manageability** Remove subcategory

**i** 12 of 14 settings in this subcategory are not configured

Microsoft Edge management enrollment token (Device)  ✓

Microsoft Edge management enrollment token  Enabled ⊖

# Understanding the Enrollment Token



What it is:

- ◆ A Policy ID string (unique identifier for a cloud policy)
- ◆ Deployed via the EdgeManagementEnrollmentToken policy setting
- ◆ Acts as a persistent pointer (device always retrieves that cloud policy)

Only one token per device (deploying a second overwrites the first)

# Policy Precedence (When Conflicts Occur)

Precedence order (highest to lowest)

1. Mandatory policies ALWAYS beat Recommended policies, regardless of source (Platform vs Cloud)
2. Platform policy ( Intune / GPO)
3. Cloud Policy Edge Management Service - Device Policy (via enrollment token)
4. Cloud Policy Edge Management Service - User Policy (via group assignment)



# Policy Precedence (When Conflicts Occur)

- ♦ Mandatory policies ALWAYS beat Recommended policies, regardless of source (Platform vs Cloud)

Microsoft Edge Policies

Policy Name	Policy Value	Source	Applies To	Level	Status	Show More
<a href="#">HomepageLocation</a>	https://google.com	Cloud token	Device	Mandatory	Warning, Conflict	^
	Value https://google.com					
	Warning More than one source with conflicting values is present for this policy!					
	Conflict https://cloudway.com	Platform	Device	Recommended		

# Policy Precedence (When Conflicts Occur)

- ◆ Mandatory policies ALWAYS beat Recommended policies, regardless of source (Platform vs Cloud)

Microsoft Edge Policies

Policy Name	Policy Value	Source	Applies To	Level	Status	Show More
<a href="#">HomepageLocation</a>	https://google.com	Cloud token	Device	Mandatory	Warning, Conflict	^
	Value https://google.com					
	Warning More than one source with conflicting values is present for this policy!					
	Conflict https://cloudway.com	Platform	Device	Recommended		

- ◆ Platform policy ( Intune / GPO) beat Cloud Policy

Microsoft Edge Policies

Policy Name	Policy Value	Source	Applies To	Level	Status	Show More
<a href="#">HomepageLocation</a>	https://cloudway.com	Platform	Device	Recommended	Warning, Conflict	^
	Value https://cloudway.com					
	Warning More than one source with conflicting values is present for this policy!					
	Conflict https://google.com	Cloud token	Device	Recommended		

# Override Policy Precedence

## Within Edge Management Service:

- ◆ Device policy wins over user policy (by default)
- ◆ Can be reversed with **EdgeManagementUserPolicyOverridesCloudMachinePolicy** registry setting

```
reg add HKLM\Software\Policies\Microsoft\Edge /v  
EdgeManagementUserPolicyOverridesCloudMachinePolicy /t REG_DWORD  
/d 1
```

# Override Policy Precedence

<a href="#">ShowHomeButton</a>	false	Platform	Current user	Mandatory	Warning, Conflict
Value	false				
Warning	More than one source with conflicting values is present for this policy!				
Conflict	true	Cloud	Current user	Mandatory	

To make Edge cloud policies override GPO/Intune:

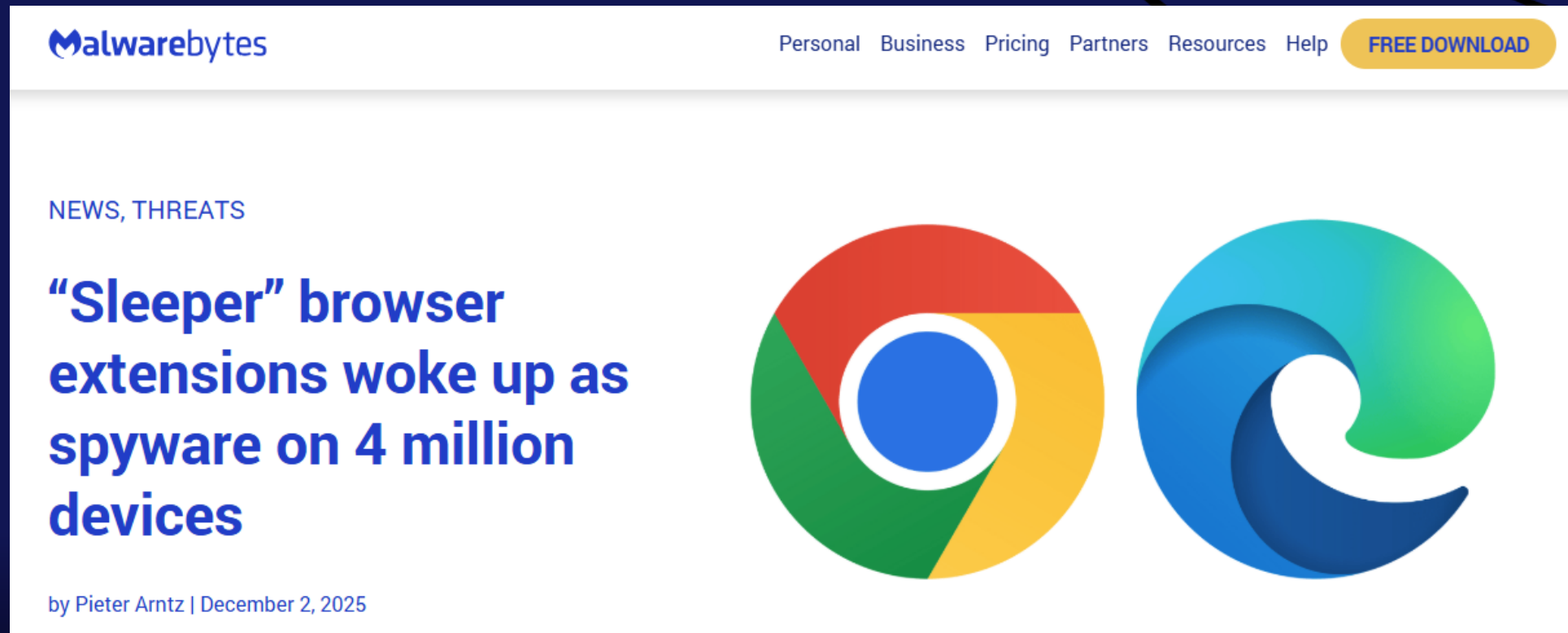
- ◆ Set **EdgeManagementPolicyOverridesPlatformPolicy** registry setting
- ```
reg add HKLM\Software\Policies\Microsoft\Edge /v  
EdgeManagementPolicyOverridesPlatformPolicy /t REG_DWORD /d 1
```

# Extension Management



# Edge extensions - security

- ◆ Extensions = any other software you run on your machine

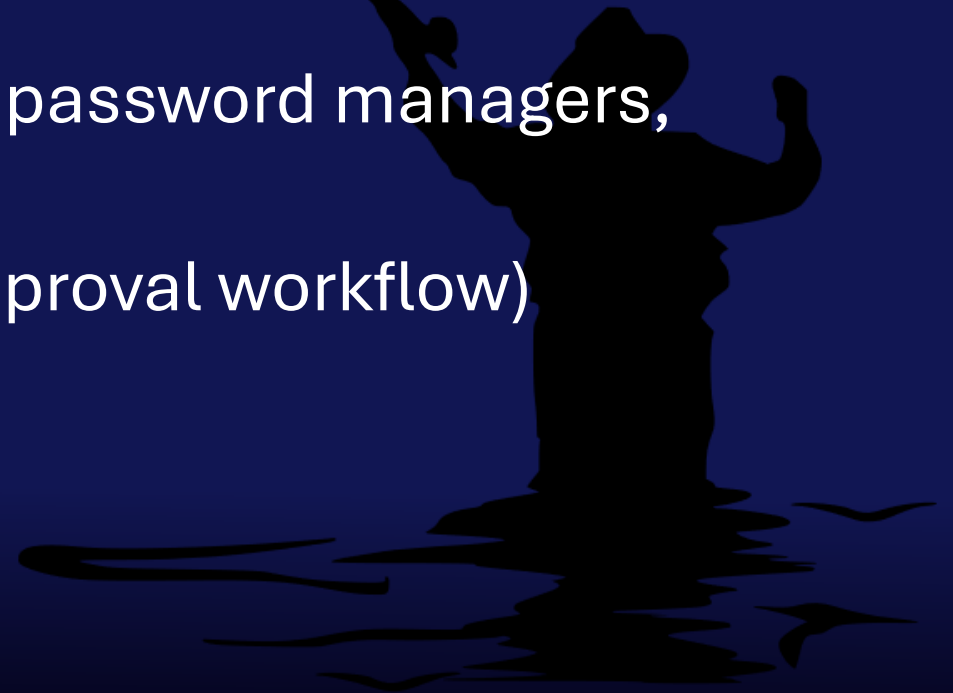


The screenshot shows the Malwarebytes website header with navigation links: Personal, Business, Pricing, Partners, Resources, Help, and a yellow 'FREE DOWNLOAD' button. Below the header, the text 'NEWS, THREATS' is displayed. The main article title is **“Sleeper” browser extensions woke up as spyware on 4 million devices**. To the right of the title are the logos for Google Chrome and Microsoft Edge. At the bottom left of the article preview, it says 'by Pieter Arntz | December 2, 2025'.

<https://www.malwarebytes.com/blog/news/2025/12/sleeper-browser-extensions-woke-up-as-spyware-on-4-million-devices>

# Extension Management Capabilities

- ◆ Extension inventory (see what's installed across your organization)
- ◆ Block all extensions (allowlist or blocklist approach)
- ◆ Control extension installation sources (Microsoft Edge Add-ons store only, sideloading control)
- ◆ Force-install corporate extensions (e.g., password managers, security tools)
- ◆ User extension requests (self-service approval workflow)



# Extension Monitoring

Home > Microsoft Edge for Business

## Microsoft Edge for Business

[Monitoring dashboard](#) ▾ [Configuration policies](#) [Site lists](#) [Connectors](#) [Copilot](#) [Resources](#)

[Provide Feedback](#)

### Extensions Monitoring

NOT ENABLED

Requested extensions

N/A

Enable to see content

# Extension Monitoring

## Enable your Dashboard

The monitoring dashboard provides further insights into your managed browsers, helping you proactively manage and optimize Edge for Business in your organization.

This will send a limited set of Edge diagnostic data to Microsoft. You may also choose to configure necessary policies to enable additional features. Please note that data may take up to 24 hours to populate once enabled.

- Enable monitoring dashboard**  
Send optional diagnostic data to Microsoft  On
- Share page URL data**  
Optionally share for enhanced browsing and search  Off
- Security Insights**  
Easily manage updates for out-of-date devices  On
- Extensions Monitoring**  
View installed extensions across your managed browsers  Off

## Enable your Dashboard

The monitoring dashboard provides further insights into your managed browsers, helping you proactively manage and optimize Edge for Business in your organization.

This will send a limited set of Edge diagnostic data to Microsoft. You may also choose to configure necessary policies to enable additional features. Please note that data may take up to 24 hours to populate once enabled.

- Enable monitoring dashboard**  
Send optional diagnostic data to Microsoft  On
- Share page URL data**  
Optionally share for enhanced browsing and search  Off
- Security Insights**  
Easily manage updates for out-of-date devices  On
- Extensions Monitoring**  
View installed extensions across your managed browsers  On

# Extension Monitoring

Home > Microsoft Edge for Business

## Microsoft Edge for Business

[Extensions monitoring](#) ▾ [Configuration policies](#) [Site lists](#) [Connectors](#) [Copilot](#) [Resources](#)

*Note: We have recently updated this page to aggregate all extension requests. You may temporarily see previously resolved requests.*

[↑ Export](#)

Active extension requests - 0  
You do not have any active extension requests.

Resolved extension requests - 0

[View resolved requests](#)

[↑ Export](#)

All installed extensions - 4

| Extension name ↑                                                         | Users with extension installed |
|--------------------------------------------------------------------------|--------------------------------|
| ChatGPT Widescreen                                                       | 1                              |
| Doubao Chat Assistant - Help You Quickly Locate Historical Conversations | 1                              |
| Google Docs Offline                                                      | 1                              |
| Unblocked Games 6x                                                       | 1                              |

### ChatGPT Widescreen

Manage active requests and view information for this extension.

[Extension details](#)

Extension ID  
obnaaalnokmchdoagnhmlakacaaooa [Copy ID to clipboard](#)

Description  
Enhances ChatGPT with wide/full/tall-screen + spamblock modes. Also works on poe.com

# Request extensions

- ◆ Extensions are hard to manage, information security, GDPR...
- ◆ Instead of blocking and allowing we can allow the end-user to request an extension!

Home > Microsoft Edge for Business > Create policy configuration

### Create a configuration policy for Microsoft Edge

- ✓ Basics
- ✓ Settings
- Extensions
- Assignments
- Finish

#### Default extension settings

These are the default settings for all extensions in this policy. You will be able to override these defaults for managed extensions. [Learn more about match patterns](#) and [permissions for extensions](#).

#### Installation settings

Allow these types of apps and extensions:

|                     |                                                  |
|---------------------|--------------------------------------------------|
| Extension           | ▼                                                |
| External extensions | Block external extensions from being installed ▼ |
| Install sources     | Not configured ▼                                 |

#### Permissions and URLs

|               |                  |
|---------------|------------------|
| Blocked hosts | Not configured ▼ |
| Allowed hosts | Not configured ▼ |

#### Blocked extensions

|                                |                                             |
|--------------------------------|---------------------------------------------|
| Extension requests ⓘ           | Allow users to request blocked extensions ▼ |
| Unmanaged extensions           | Block all unmanaged extensions by default ▼ |
| Block extensions by permission | Not configured ▼                            |

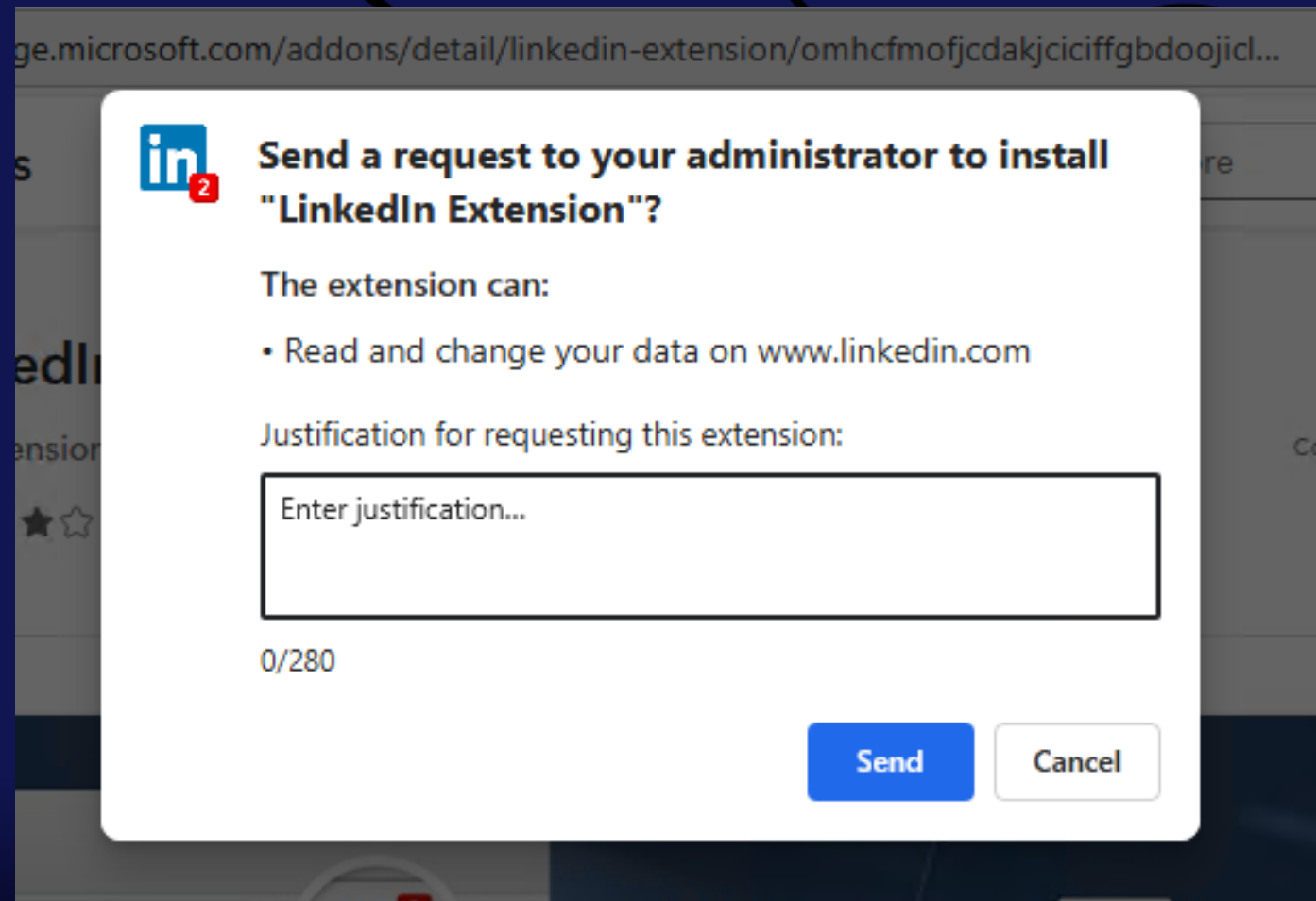
#### Message for users when extension is blocked

Example: Your IT admin has blocked this extension

0/1000 characters



# Request extensions

- ◆ Extensions are hard to manage, information security, GDPR...
- ◆ Instead of blocking and allowing we can allow the end-user to request an extension!



Extensions

Requests

 Manage request settings  Refresh

|                          | Name ↑                                          | Number of requests | Last requested       |
|--------------------------|-------------------------------------------------|--------------------|----------------------|
| <input type="checkbox"/> | 1Password – Password Manager                    | 2                  | 2025-07-07, 09:47:52 |
| <input type="checkbox"/> | AdBlock — block ads across the web              | 1                  | 2025-07-07, 09:29:08 |
| <input type="checkbox"/> | Add to Microsoft To Do                          | 1                  | 2025-07-07, 09:28:08 |
| <input type="checkbox"/> | Microsoft 50th Anniversary –<br>Celebration     | 1                  | 2025-07-07, 09:28:35 |
| <input type="checkbox"/> | Microsoft Bing Homepage and<br>Search Engine    | 1                  | 2025-07-08, 14:39:00 |
| <input type="checkbox"/> | Microsoft Bing Search Engine                    | 1                  | 2025-07-07, 09:27:46 |
| <input type="checkbox"/> | Microsoft Editor: Spelling &<br>Grammar Checker | 1                  | 2025-07-07, 09:47:14 |
| <input type="checkbox"/> | OneNote Web Clipper                             | 1                  | 2025-07-07, 09:28:20 |

# Allow Extensions based on permissions

- ◆ Block extensions based on permissions
- ◆ Simplifies management to allow extensions based on permissions

Block extensions by permission

Block extensions that require selected permissions

Users will not be able to install or use extensions: managed extensions to allow them if they require

Block extensions that require selected permissions

Not configured

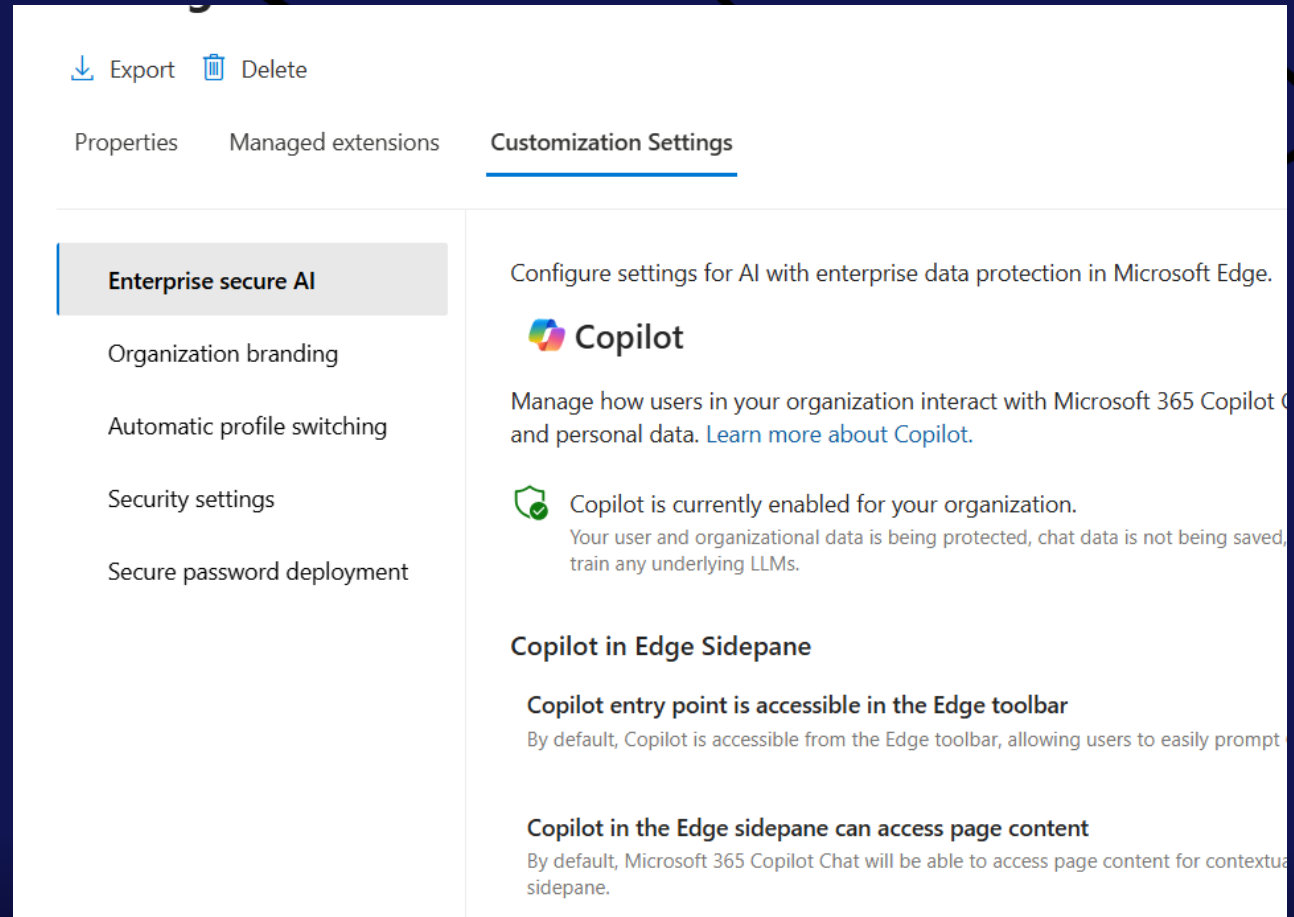
Search

Permission ↑

None selected

# Customization settings

- ◆ Enterprise secure AI
- ◆ Organisation branding
- ◆ Automatic profile switching
- ◆ Security settings
- ◆ Secure password deployment



The screenshot shows the 'Customization Settings' page in Microsoft Edge. At the top, there are 'Export' and 'Delete' buttons. Below that are three tabs: 'Properties', 'Managed extensions', and 'Customization Settings', with the latter being the active tab. A left-hand navigation pane lists several settings: 'Enterprise secure AI' (highlighted), 'Organization branding', 'Automatic profile switching', 'Security settings', and 'Secure password deployment'. The main content area is titled 'Configure settings for AI with enterprise data protection in Microsoft Edge.' and features the 'Copilot' logo. Below the logo, it states: 'Manage how users in your organization interact with Microsoft 365 Copilot and personal data. [Learn more about Copilot.](#)' A green shield icon indicates that 'Copilot is currently enabled for your organization.' and provides details: 'Your user and organizational data is being protected, chat data is not being saved, and Copilot will not train any underlying LLMs.' Further down, there are sections for 'Copilot in Edge Sidepane' with two sub-sections: 'Copilot entry point is accessible in the Edge toolbar' (noted as default) and 'Copilot in the Edge sidepane can access page content' (noted as default).

# Enterprise Secure AI

<https://bard.google.com>, <https://chat.openai.com>, <https://chatgpt.com>,  
<https://chatgpt.es>,  
<https://gemini.google.com>, <https://claude.ai>  
<https://perplexity.ai>, <https://jasper.ai>, <https://you.com>,  
<https://writesonic.com/chat>, <https://cohere.com/coral>, <https://deepseek.com>,  
<https://deepseek.me>

## Other AI features

Manage additional AI features to protect your company and user data.

### Users can access third-party LLM chatbots

By default, users will be able to access most major LLM-based chatbot sites other than Copilot.

Policy applies to \*

Windows  macOS  iOS  Android

Only a subset of LLM chatbots  
are currently blocked

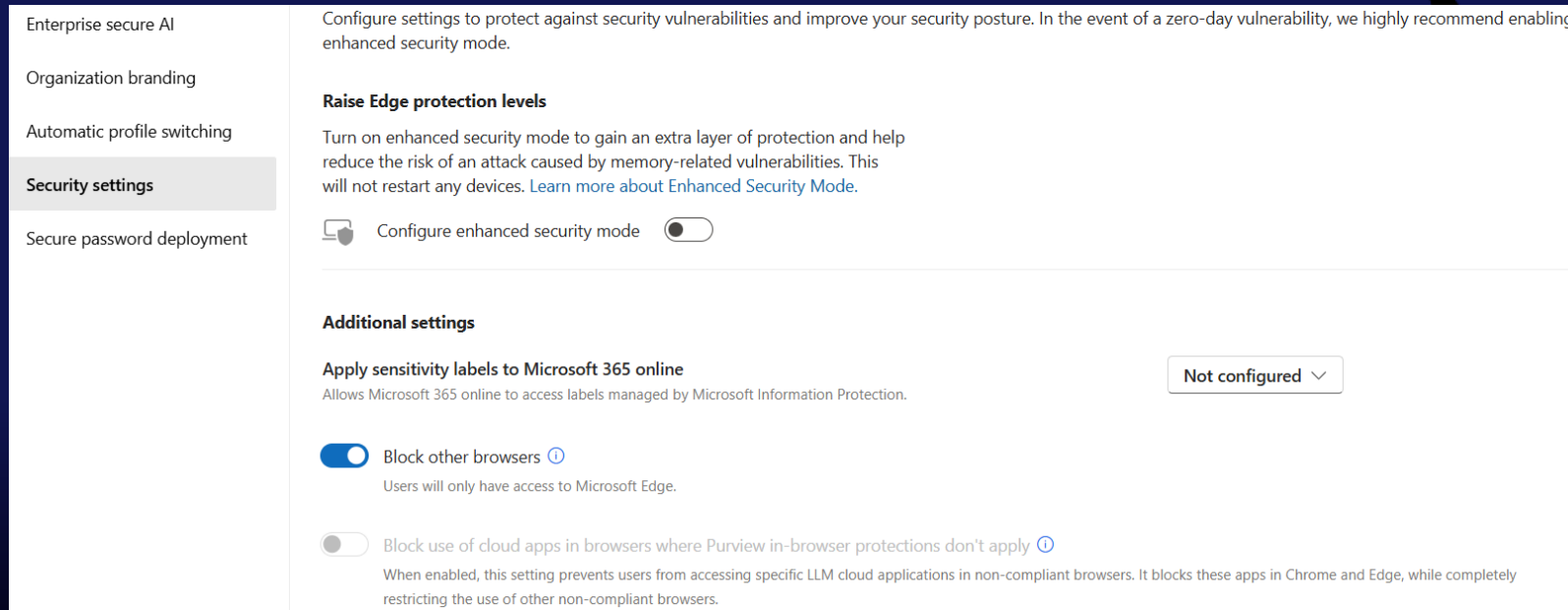
Block all



Disabled ▾

# Block “other” Browsers

- ◆ Creates an AppLocker policy in Intune
- ◆ Both Executables and Store apps
- ◆ Requires Intune License



The screenshot shows the Microsoft Intune Security settings page. The left sidebar contains navigation options: Enterprise secure AI, Organization branding, Automatic profile switching, Security settings (highlighted), and Secure password deployment. The main content area is titled 'Configure settings to protect against security vulnerabilities and improve your security posture. In the event of a zero-day vulnerability, we highly recommend enabling enhanced security mode.' It features a section for 'Raise Edge protection levels' with a toggle for 'Configure enhanced security mode' which is currently turned off. Below this is an 'Additional settings' section with a dropdown menu set to 'Not configured'. The 'Block other browsers' setting is turned on, with a sub-note: 'Users will only have access to Microsoft Edge.' The 'Block use of cloud apps in browsers where Purview in-browser protections don't apply' setting is turned off, with a sub-note: 'When enabled, this setting prevents users from accessing specific LLM cloud applications in non-compliant browsers. It blocks these apps in Chrome and Edge, while completely restricting the use of other non-compliant browsers.'

Enterprise secure AI

Organization branding

Automatic profile switching


**Security settings**

Secure password deployment

Configure settings to protect against security vulnerabilities and improve your security posture. In the event of a zero-day vulnerability, we highly recommend enabling enhanced security mode.

**Raise Edge protection levels**

Turn on enhanced security mode to gain an extra layer of protection and help reduce the risk of an attack caused by memory-related vulnerabilities. This will not restart any devices. [Learn more about Enhanced Security Mode.](#)

 Configure enhanced security mode

**Additional settings**

**Apply sensitivity labels to Microsoft 365 online** Not configured ▾

Allows Microsoft 365 online to access labels managed by Microsoft Information Protection.

**Block other browsers** ⓘ

Users will only have access to Microsoft Edge.

**Block use of cloud apps in browsers where Purview in-browser protections don't apply** ⓘ

When enabled, this setting prevents users from accessing specific LLM cloud applications in non-compliant browsers. It blocks these apps in Chrome and Edge, while completely restricting the use of other non-compliant browsers.

# Blocked Browsers

- ◆ Opera
- ◆ Google Chrome
- ◆ FireFox
- ◆ Brave
- ◆ Vivaldi
- ◆ Tor Browser
- ◆ Puffin Secure Browser
- ◆ UC Browser
- ◆ Wave Browser
- ◆ DuckDuck GO

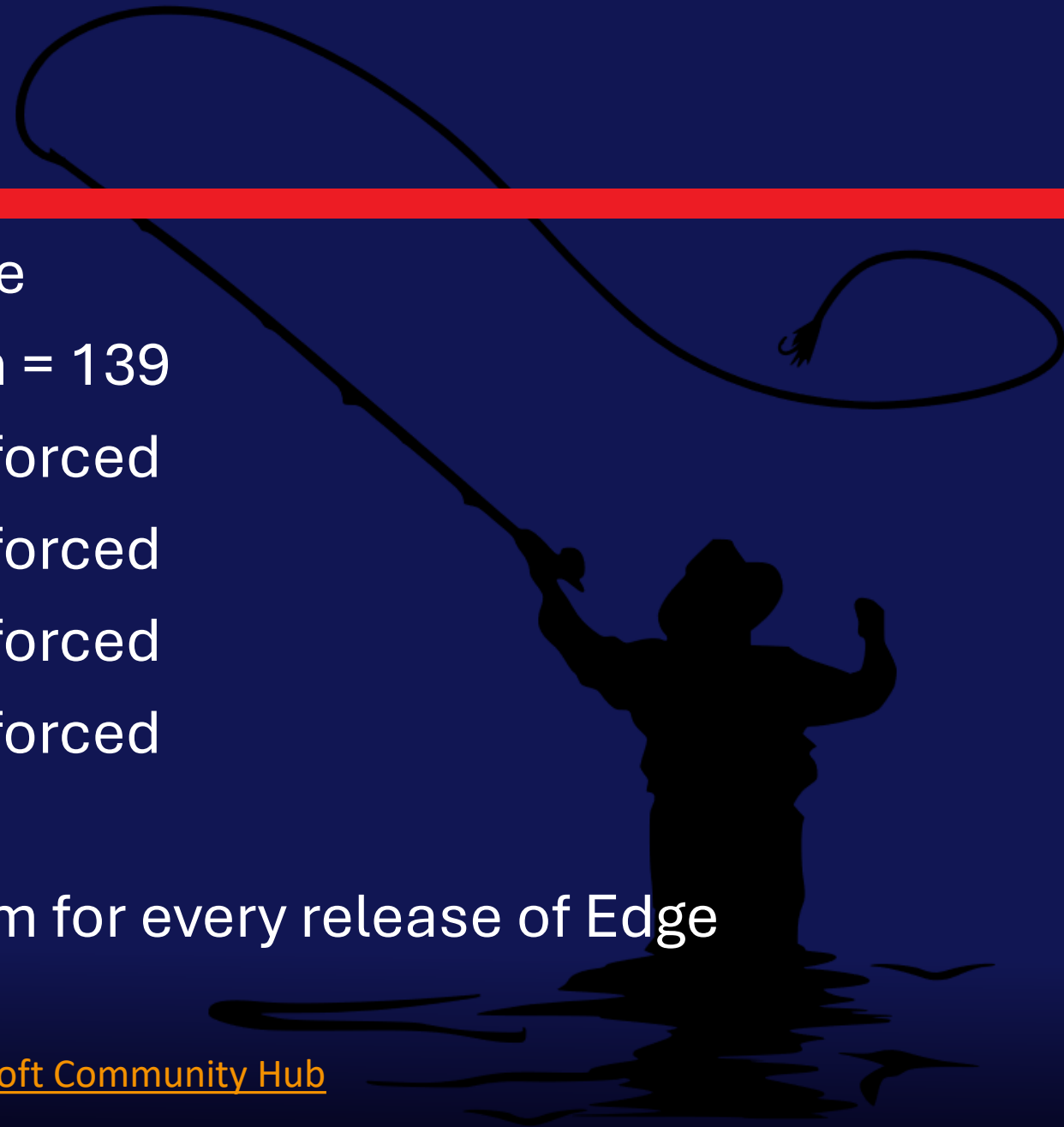
```
1 <RuleCollection Type="Exe" EnforcementMode="Enabled">
2   <FilePublisherRule Id="06fdf5f2-4434-4b6b-b836-59dc1ee29b80">
3     <Conditions>
4       <FilePublisherCondition PublisherName="O=OPERA NORWAY AS">
5         <BinaryVersionRange LowSection="*" HighSection="*" />
6       </FilePublisherCondition>
7     </Conditions>
8   </FilePublisherRule>
9   <FilePublisherRule Id="10d0ad50-5220-4ae7-b23a-fb2c81d75610">
10    <Conditions>
11      <FilePublisherCondition PublisherName="O=GOOGLE LLC, L">
12        <BinaryVersionRange LowSection="*" HighSection="*" />
13      </FilePublisherCondition>
14    </Conditions>
15  </FilePublisherRule>
16  <FilePublisherRule Id="14a0952e-e740-4f5b-9983-68fb308a9a40">
17    <Conditions>
18      <FilePublisherCondition PublisherName="O=OPERA NORWAY AS">
19        <BinaryVersionRange LowSection="*" HighSection="*" />
20      </FilePublisherCondition>
```

# Security Baselines

- ◆ Reviewed for each version of Edge
- ◆ Current Security Baseline version = 139
- ◆ Version 140 – no new settings enforced
- ◆ Version 141 – no new settings enforced
- ◆ Version 142 – no new settings enforced
- ◆ Version 143 – no new settings enforced

Subscribe to changes – review them for every release of Edge

[Microsoft Security Baselines Blog](#) | [Microsoft Community Hub](#)

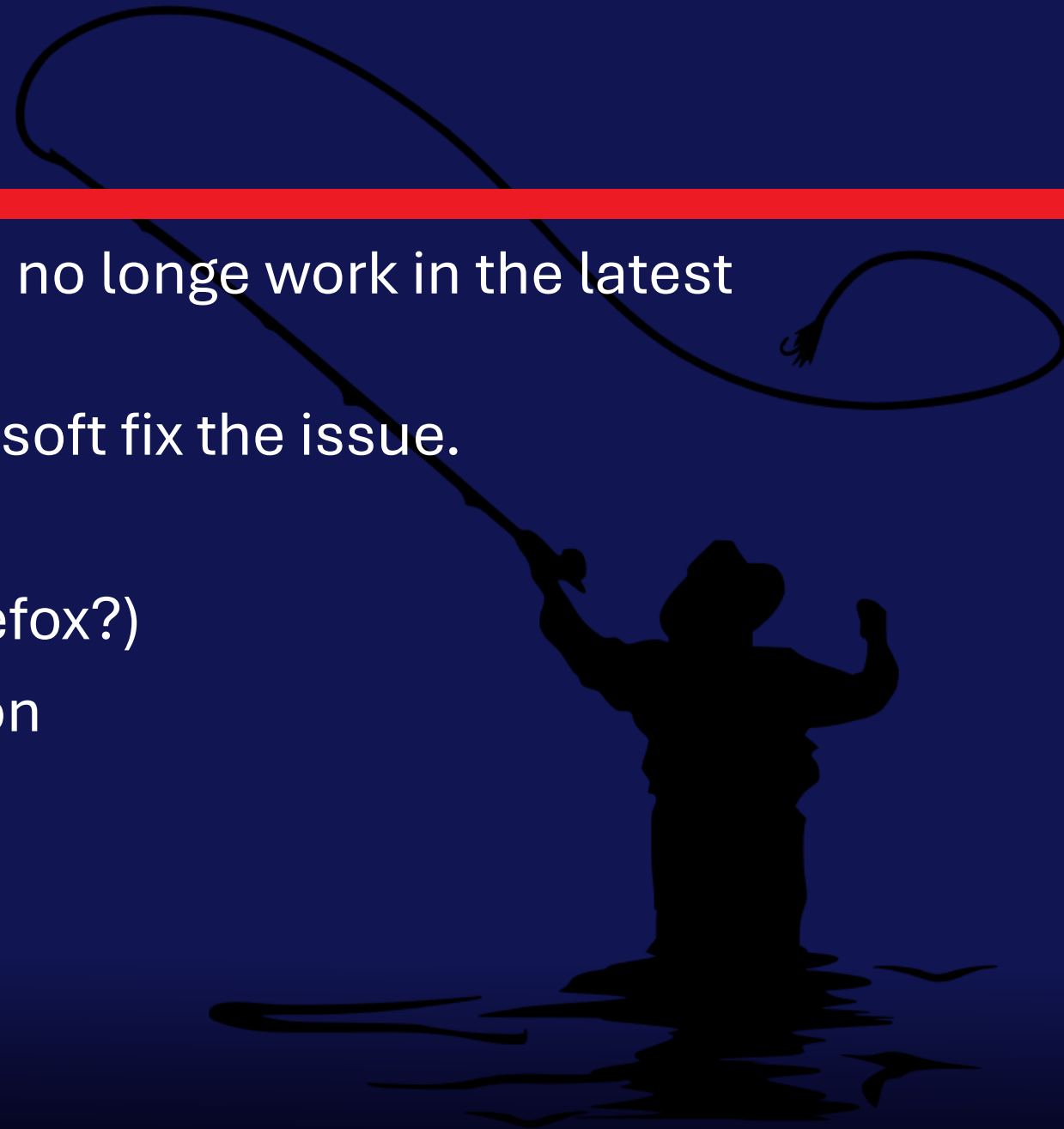


# Rollback plan

- ◆ What happens if the CRM system no longer works in the latest release of Edge?
- ◆ Will take some days before Microsoft fix the issue.

## Solution:

- ◆ Deploy a secondary browser (Firefox?)
- ◆ Rollback Edge to a working version








# Rollback settings




- ◆ Tr
- ◆ Sy



**Applications > Microsoft Edge** Remove subcategory




**i** 15 of 20 settings in this subcategory are not configured

Update policy override    Enabled 

Policy (Device)  \*  

Target version override    Enabled 

Target version (Device)   

Rollback to Target version    Enabled 

# Policy sync - Intervals

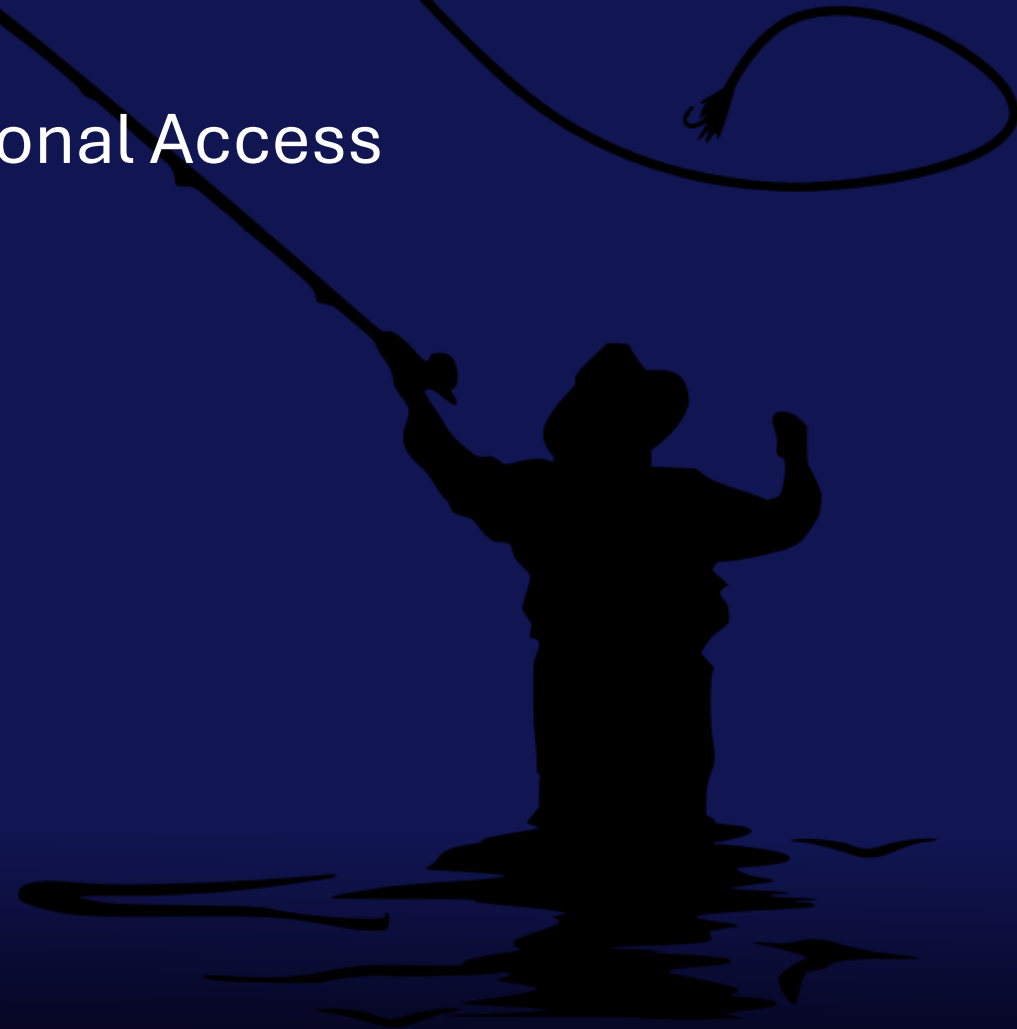
- ◆ When a user signs into Microsoft Edge on a device for the first time
- ◆ Check for changes every 90 minutes.
- ◆ If there aren't any changes to the configuration policy since the last check, another check is made again in 24 hours.
- ◆ If there's an error, a check is made when the user opens Microsoft Edge.
- ◆ If Microsoft Edge isn't running when the next check is scheduled, then the check will be made the next time the user opens Microsoft Edge.

# B2B and BYOD support



# Bring your own device (Windows)

- ◆ Use App Protection policy
- ◆ Require App Protection policy in Conditional Access
- ◆ Edge policies applies when user sign-in
  - ◆ We can control extensions
  - ◆ Security settings
  - ◆ Control access to AI in the Edge session
  - ◆ Security Baseline



# Supported Scenarios and Known Limitations

The device-level Endpoint DLP block can be bypassed using the policy MAMWithDeviceDLPEEnabled. This policy must be configured by the tenant managing the device

<https://learn.microsoft.com/en-us/deployedge/microsoft-edge-cross-tenant-support-using-intune-mam#supported-scenarios-and-known-limitations>

| Limitation                     | Impact                                                                                                                                                                                                                                                                                   |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Same-tenant managed devices    | Devices managed by the <b>same tenant</b> aren't supported with the Conditional Access configuration described in this article. Users can't access Conditional Access-protected data in this configuration.                                                                              |
| Endpoint DLP enabled on device | If <b>device level Endpoint DLP</b> is enabled, Intune App Protection (MAM) policies cannot be applied to Edge work profiles on that device unless a policy is set to bypass this limitation. Otherwise, profile switching will not be available, and the added profile must be removed. |

## How to verify whether Endpoint DLP is enabled on a device

1. Open Microsoft Edge
2. Navigate to `edge://edge-dlp-internals`
3. On the Feature Status page, check the **Provider Name** field

If the **Provider State** is set to **Available** and the provider is **Endpoint DLP**, device-level Endpoint DLP is enabled.

## Microsoft Edge Application Management

Your work account has been blocked due to device management

Your device is managed with a device protection policy, which prevents app protection from being applied for jonil2@demiranda.nu.

Contact the administrator for the account/resource you're trying to access, or use a device that supports app protection.

Remove Account

Close

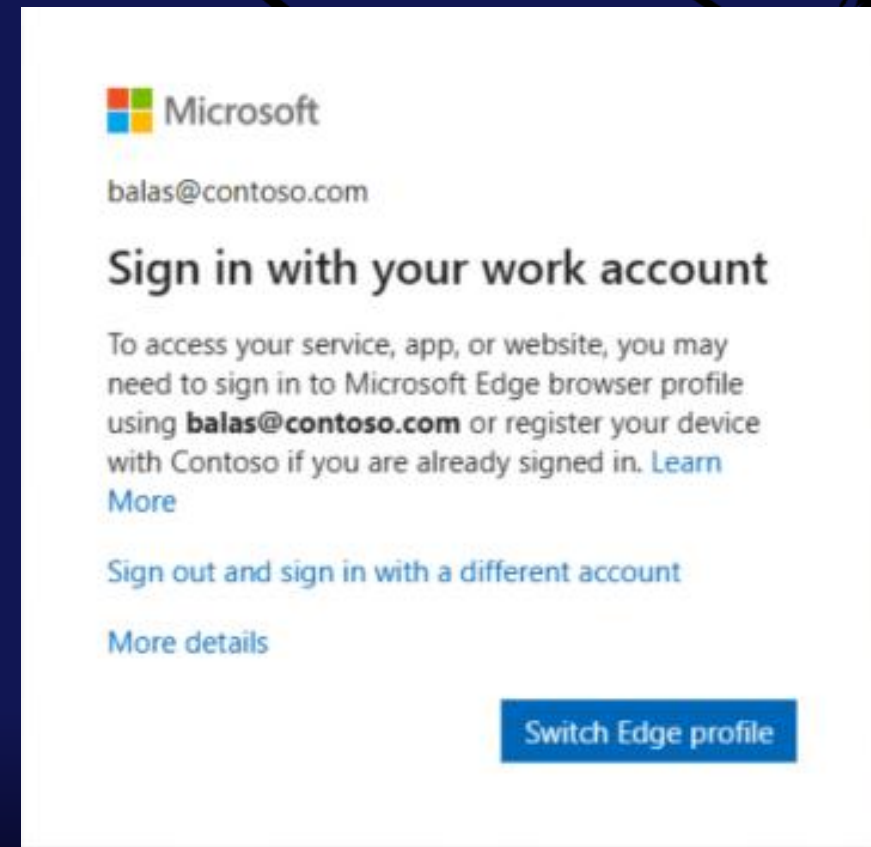
# App protection policy for Edge

- ◆ Used to configure privacy settings in Edge for BYOD devices
- ◆ Privacy control:
  - ◆ Receive data from
  - ◆ Send org data to
  - ◆ Allow cut, copy, and paste
  - ◆ Printing org data
- ◆ Launch Control:
  - ◆ Version, offline control...



# Conditional Access – Force sign in

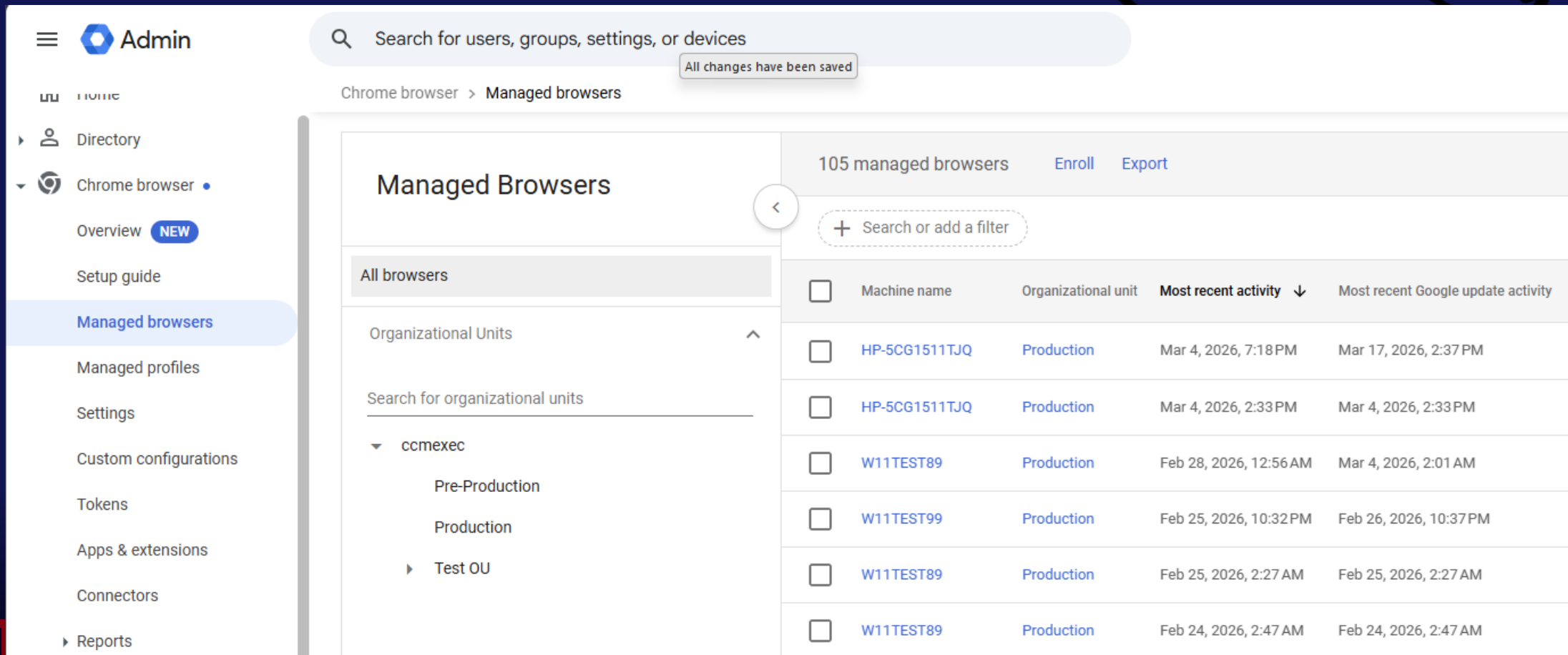
- ◆ For BYOD devices we can require App Protection using conditional access.
- ◆ If a user has not signed in Edge will receive a message that they must sign in.



A silhouette of a cowboy standing in water, holding a lasso that is looped in the air. The cowboy is wearing a hat and boots. The lasso is a long rope with a fringed end, forming a large loop in the air. The cowboy's reflection is visible in the water below him.

# What about Google Chrome?!

# Same functionality - free



Admin

Search for users, groups, settings, or devices

All changes have been saved

Chrome browser > Managed browsers

## Managed Browsers

105 managed browsers [Enroll](#) [Export](#)

+ Search or add a filter

| <input type="checkbox"/> | Machine name  | Organizational unit | Most recent activity ↓ | Most recent Google update activity |
|--------------------------|---------------|---------------------|------------------------|------------------------------------|
| <input type="checkbox"/> | HP-5CG1511TJQ | Production          | Mar 4, 2026, 7:18 PM   | Mar 17, 2026, 2:37 PM              |
| <input type="checkbox"/> | HP-5CG1511TJQ | Production          | Mar 4, 2026, 2:33 PM   | Mar 4, 2026, 2:33 PM               |
| <input type="checkbox"/> | W11TEST89     | Production          | Feb 28, 2026, 12:56 AM | Mar 4, 2026, 2:01 AM               |
| <input type="checkbox"/> | W11TEST99     | Production          | Feb 25, 2026, 10:32 PM | Feb 26, 2026, 10:37 PM             |
| <input type="checkbox"/> | W11TEST89     | Production          | Feb 25, 2026, 2:27 AM  | Feb 25, 2026, 2:27 AM              |
| <input type="checkbox"/> | W11TEST89     | Production          | Feb 24, 2026, 2:47 AM  | Feb 24, 2026, 2:47 AM              |

Organizational Units

Search for organizational units

- ccmexec
  - Pre-Production
  - Production
    - Test OU

# Google Chrome Management

- ◆ Token per Organization unit
- ◆ Deploy token using Intune
- ◆ Configure per device

Configuration settings [Edit](#)

^ Google

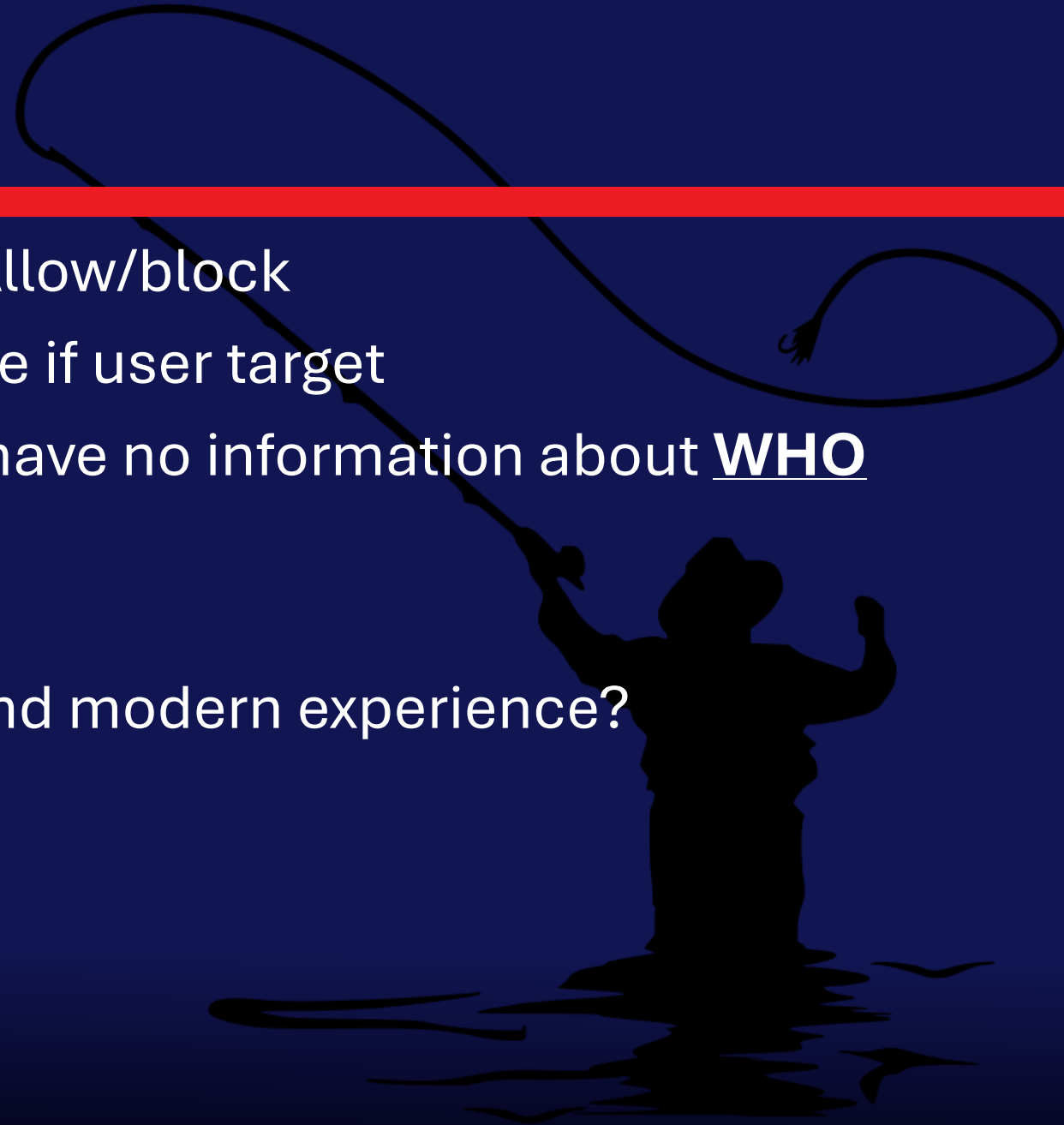
## Google Chrome

The enrollment token of cloud policy on desktop (Device) 15efd489-203e-4747-bfcb-914cd30cf70f

The enrollment token of cloud policy on desktop Enabled

# Lessons learned

- ◆ Browser strategy is necessary – Allow/block
- ◆ Requires force user sign in in Edge if user target
- ◆ When requesting extensions we have no information about WHO requested it.
- ◆ Time to move to a more secure and modern experience?



# SAVE THE DATES

Oct 25-28, 2026



May 2-6, 2027



Oct 10-13, 2027



# Extended Q&A



2Pint

Recast

robopack  
empowered by SOFTWARE CENTRAL

SquaredUp

CODETWO

baramundi

ninjaOne

Rimo3



TeamViewer

numecent

aiden